USS THE SULLIVANS (DDG 68)

WEARABLE PC & WIRELESS LAN

ELECTROMAGNETIC INTERFERENCE AND THREAT ANALYSIS TEST REPORT

PREPARED FOR:

PEO TAD/SC
2531 JEFFERSON DAVIS HWY
ARLINGTON, VA 22202

PREPARED BY:

15800 CRABBS BRANCH WAY
ROCKVILLE, MD 20855
(301) 670-6770

AUTHORS:
BENGA ERINLE (erinle@aeptec.com)
RUSSELL DOMINIQUE (dominique@aeptec.com)

OCTOBER 15, 1998

EXECUTIVE SUMMARY

In August 1997, PEO TAD/SC received a congressional plus up of $3 Million "to gain at-sea experience with combined IETM/Wearable Computer system". This effort required integrating The Wearable Computer and a Wireless LAN aboard Surface Combatants to gain such experience. Program objectives were aimed to provide ships force with capabilities that included mobile digitization, robust computer/video/voice platform, and a Wireless LAN (WLAN) for performance of operational duties anywhere within ship. Such capabilities would support the Smart Ship Project goal to "install and maintain innovative projects… and demonstrate the resulting reductions in manpower and benefits associated with life-cycle costs." AEPTEC Microsystems, Inc. was tasked to be the systems integrator and to implement the program objectives. These objectives included:

- Providing sailors access to IETMs via the Wearable PC.
- Enhancing operational effectiveness of sailors by utilizing the Wearable PC as a platform for launching other operational applications sets including CSOSS at the point of need within the ship's hull.
- Integrating COTS technologies that enhance the capabilities of the Wearable PC including VTC and Virtual Test Equipment for technical assistance.
- Providing a Wireless extension to the Unclassified LANs on PEO TAD/SC ships to facilitate un-tethered operation of the Wearable PC.

The first aspect of the program was to conduct EMI and Threat Analysis testing of WLAN emissions. The WLAN system is a frequency hopping spread spectrum designed to provide ship-wide RF connectivity to the unclassified LAN. The system operates between 2.4 and 2.5 GHz at power levels of 100 milli-Watts (mW) and 500 mW. This report documents the findings of the EMI tests.

PMS 400F selected USS The Sullivans (DDG 68) as the EMI Test Platform in February 1998. In April 1998, the WLAN system was installed aboard DDG 68. The installed system comprised of 27 Wireless Hubs (radiating at 500 mW) and 25 Wearable PCs (with RF LAN cards radiating at 100 mW). A total of 5 additional RF LAN Cards were provided to DDG 68 officers for use in Laptop computers. The Wearable PCs were configured with applications including Electronic CSOSS, FCS IETM, SIB IETM, and Microsoft NetMeeting (for remote tech-assists). System testing began at DDG 68's homeport of Mayport, Florida in April 1998 and continued through July 1998. System testing included both pier-side and at-sea testing. The tests conducted during this effort were informal tests conducted within the scope of the systems integration effort. The results of the testing are identical to results obtained by SURFPAC during the 1996 Single Pipeline demonstrations that included a similar WLAN system.

At the conclusion of the testing, the WLAN coverage proved to be ship-wide except for voids, fan room, and tanks. In the Aft section of the ship between Frame 350 and 420, coverage was determined to be "spotty". To improve coverage in these areas, 3 additional Access Points were added in August 1998 which corrected the coverage problem. With regards to electromagnetic susceptibility by ship systems, no EMI incidents were reported during the test period nor have any been reported to date. The Threat Analysis portion of the tests also revealed no increased threat due to WLAN RF emissions. Threat Analysis tests were conducted by the SESEF in Mayport, Florida in June 1998.

BACKGROUND

TEST OBJECTIVES

The objectives of this effort was to perform tests and/or procedures to assess the following:

1. Shipboard WLAN coverage.
2. Electromagnetic susceptibility of shipboard systems to the WLAN.
3. Ship detectability due to WLAN emissions.

The Test Plan for this effort was submitted to PMS 400D and PMS 400F in April 1998. That plan is included later in this report.

WIRELESS LAN TECHNOLOGY

The Wireless LAN uses Spread Spectrum technology. This is the art of secure digital communications that is currently being exploited for commercial and industrial purposes. Spread Spectrum uses wide-band, noise-like signals that are inherently difficult to detect. Spread Spectrum signals are also difficult to intercept or demodulate. Further, they are more difficult to jam (interfere with) than narrow-band signals. These Low Probability of Intercept (LPI) and anti-jam (AJ) features are why the military has used Spread Spectrum for so many years. Spread signals are intentionally made to be much wider band than the information they carry to make them appear noise-like. Spread Spectrum transmitters use similar transmit power levels as narrow band transmitters, but because their signals are so wide, they transmit at a much lower spectral power density than narrow-band transmitters. This lower transmitted power density characteristic makes spread signals attractive for use in applications such as shipboard networking. Spread Spectrum signals and narrow-band signals (or noise) can occupy the same band, with little or no interference. This capability is the main reason for all the interest in Spread Spectrum today.

The Wireless LAN implements spread spectrum communication via the frequency hopping method. Each Access Point, which connects to the wired LAN backbone, executes a unique hopping pattern across 78 non-overlapping frequencies. The table of 66 hopping patterns specified in the IEEE 802.11 standard minimizes the probability that one cell will operate on the same frequency at the same time as another cell. The result is several access points operating at one/two Mbps without interruption even when in close proximity to one another. In addition, Access Points can be added to expand capacity in the same geographic area as well as to extend range.

The Wireless LAN is based on a simple bridge architecture that provides transparent wireless connection to an Ethernet LAN through multiple Access Points. The full cellular network supports seamless, instantaneous roaming with load balancing. Mobile stations communicate through a PCMCIA adapter with an integrated antenna. Each adapter is equipped with industry standard network device drivers, and Access Points are compatible with the Simple Network Management Protocol (SNMP). Open standards at every hardware and software interface allows seamless integration into existing wired networks such as SNAP III and IT-21.

TEST PLAN

The following is the WLAN EMI and Threat Analysis test plan as implemented on DDG 68. This test plan was developed based on the WLAN installation on DDG 68 as of April 1998. The plan was implemented by AEPTEC Microsystems personnel, DDG 68 crew, and Mayport SESEF representatives.

WIRELESS COVERAGE AND SUSCEPTIBILITY TESTS

1. Identify WLAN coverage, location of coverage gaps or dead zones internal to the ship. This test will measure WLAN continuity by using a Wearable or Notebook PC, equipped with a Wireless Interface Card, to roam the ship and identify any area(s) where a loss of connectivity occurs. Continuity tests will consist of SNAP LAN access and the ability to effectively "ping" other stations on the SNAP LAN. For the test period, Wireless hubs (Access Points) have been located in the following spaces:

	Access Point ID
• Aft IC Gyro	41
• Auxiliary Machine Room #1	73
• Bridge (Pilot House)	3C
• Casualty Control Station (CCS)	12
• Chief Petty Officers Mess	42
• Combat Systems Equipment Room #2	1B
• Combat Systems Equipment Room #3 Annex	72
• Combat Systems Maintenance Central (CSMC)	26
• Combat Systems Office	56
• Crew Library/Learning Center	67
• Deck Department Office (BOSN Workshop)	0E
• Forward IC Gyro	5F
• Forward VLS Passageway	02
• Gas Turbine Generator Room #3	1F
• Main Engine Room #1	2D
• Main Engine Room #2	21
• Radar Room #2	2B
• Radar Room #3	6B
• Shaft Alley	4A
• Sick Bay	29
• Sonar Cooling Equipment Room	22
• Sonar Control Room	06
• Sonar Equipment Room #2	77
• Supply Department Office	36
• Supply Support Center	5B
• Tactas Hoist Room	4F
• Wardroom Passageway	63

Besides Voids and Fan Rooms, any areas lacking WLAN coverage will be documented by space numbers. These tests should be performed during normal ship operations and during General Quarters.

2. Determine topside WLAN Coverage as a result of WLAN hubs in spaces such as Pilot House, Deck Department office, and Tactas Hoist Room. These tests should be performed with the hatches in the Pilot House open and closed. All topside areas with WLAN coverage should be documented. WLAN operation topside will facilitate the use of IETMs and Just-in-time training CBTs.

3. Determine the impact of the WLAN on ships systems such as the Main Engines, Generators, Weapon Systems, Sensors, Microwave Devices, Medical Equipment, and Internal Communication devices. This effort will assess the impact of the WLAN on equipment gauges, meters, sensors, etc. All systems tested should be documented with details on the impact or lack thereof.

DETECTABILITY TEST

1. The test will determine the range of WLAN emissions outside the hull and assess the feasibility of ship detectability and, hence, vulnerability due to such UHF emissions. The test frequency will be the 2.4 to 2.5 GHz bands.

   - Can an external source detect the WLAN? At what range did such detection occur?
   - If detectable, can external source retrieve information from WLAN and/or SNAP LAN?
   - If detectable, can external source impair the performance of or shutdown the WLAN and/or SNAP LAN?
   - What is the power emitted by the WLAN at distances of 5 NM and 10 NM with: 1) only the Wireless hubs active, and 2) with Wireless Hubs, Wearable PCs and Notebook PCs with Wireless cards active? The data from this test will be compared with state-of-the-art Electronic Support Measures (ESM) capabilities to estimate the likelihood of exploitation by a hostile force.

   Note: These tests should be performed with and without WLAN operations in the Pilot House and Topside.

TEST EQUIPMENT

1. Wearable PCs equipped with WLAN interface cards.
2. Notebook computers equipped with WLAN interface cards.
3. WLAN hubs and supporting peripherals as installed in 27 spaces around the ship.
4. SNAP III LAN and File Server.

TEST RESULTS

WIRELESS LAN COVERAGE

The purpose of the WLAN coverage tests was to identify the WLAN coverage and signal strength around the ship. This data would serve as the basis for all susceptibility and detectability tests. This test measured WLAN continuity by using both a Wearable PC and a Notebook PC equipped with a RF LAN Card. The test team roamed the ship measuring the RF Relative Signal Strength Indicator (RSSI) levels and verifying SNAP LAN access. The RSSI is approximately the dB level above the receiver sensitivity. No reception (detection) of signal by the RF LAN Card results in an RSSI of 0. An RSSI level of 32 or greater is needed for reliable WLAN communication. As the RSSI level drops below 32 the number of errors and re-transmissions increases. To prevent RSSI values below 32 and hence dead zones within the ship, AEPTEC Microsystems engineered the DDG 68 WLAN to include coverage overlaps between Access Points. Such overlaps would ensure that all areas of the ship would be covered by at least one Access Point with RSSI value greater than 32. A conversion chart between RSSI level and signal strength in dB relative to a milliwatt (dBm) is provided in Table 1 below. Note that this conversion is an approximation and that such conversions are receiver dependent.

Table 1. RSSI to dBm Conversion Table.

RSSI	dBm		RSSI	dBm
0	-90		34	-70
2	-89		36	-69
4	-88		38	-68
6	-87		40	-67
8	-85		42	-66
10	-84		44	-64
12	-83		46	-63
14	-82		48	-62
16	-81		50	-61
18	-80		52	-60
20	-78		54	-59
22	-77		56	-57
24	-76		58	-56
26	-75		60	-55
28	-74		62	-54
30	-73		64	-53
32	-71		66	-52

Table 2 provides WLAN coverage data for each Access Point relative to areas of the ship. The data is presented by the Access Point number, Access Point location and ID, coverage areas by frame number, and range of Access Point RSSI measurements in each of those areas. Note that an Access Point RSSI value of 32 or greater is required for continuity with the SNAP LAN.

The data in Table 2 shows that ship-wide WLAN coverage is approximately 90% as desired. It further shows an overlap in WLAN coverage by Access Points in most areas of the ship. An analysis of the coverage shows that the WLAN signal easily penetrates bulkheads between “sections” of the ship’s superstructure. The signal is seen to further penetrate these “sections” through interconnecting hatches unless such interconnections are through Pressure Locks or Air Locks. The strength of WLAN signals that penetrate “sections” of the superstructure are stronger or weaker based on the state (open or closed) of the interconnecting hatches. A comparison of WLAN coverage during normal conditions and during General Quarters (GQ) revealed only that weaker signals (RSSI values under 45) were lost during GQ.

Table 2. WLAN Coverage Data

Hub #	Access Point Location & ID	Spaces with WLAN Coverage	Associated RSSI Values
1	**Bridge (AP ID – 3C)** **04-130-0-C**	04 Level (Frames 126 to 170) 05 Level (above Bridge) 03 Level (Frames 126 to 170) 02 Level (Frames 126 to 160) 01 Level - Topside Only (Frames 30 to 210)	50 – 63 45 – 56 38 – 56 42 – 57 33 – 50
2	**Radar Room #2 (AP ID – 2B)** **03-142-0-C**	05 Level (above Bridge) 04 Level (Frames 126 to 170) 03 Level (Frames 112 to 170) 02 Level (Frames 112 to 174 01 Level (Frames 122 to164) Main Deck (Frame 169 StarBd)	38 – 43 45 – 57 35 – 63 35 – 59 30 – 42 0 – 34
3	**Wardroom Passage (AP ID – 63)** **02-154-2-Q**	04 Level (Frames 126 to 170) 03 Level (Frames 126 to 170) 02 Level (Frames 112 to 174 01 Level (Frames 122 to 200) Topside (Frames 118 to 170) Main Deck (Frames 126 to 160)	40 – 55 33 – 56 40 – 63 35 – 55 0 – 49 28 – 53
4	**CSMC (AP ID – 26)** **01-130-0-C**	04 Level (Frames 126 to 170) 03 Level (Frames 112 to 170) 02 Level (Frames 112 to 174 01 Level (Frames 110 to174) Main Deck (Frames 78 to 169)	0 – 45 32 – 42 20 – 53 32 – 63 32 – 50
5	**Combat Systems Office (AP ID – 56)** **0.5-42-2-Q**	0.5 & 01 Level (Frames 18 to 51) Main Deck (Frames 18 to 84) 1st Platform (Frames 50 to 78)	34 – 63 43 – 55 35 – 40
6	**FWD VLS Passage (AP ID – 02)** **1-78-01-L**	02 Level (Frames 112 to 126) 0.5 & 01 Level (Frames 42 to164) Main Deck (Frames 78 to 250) 1st Platform (Frames 50 to 158) 2nd Platform (Frames 78 to 158) Hold (Frames 94 to 126)	40 - 42 34 – 47 20 – 63 20 – 53 0 – 53 34 – 43
7	**Sonar Control Rm. (AP ID – 06)** **2-50-2-C**	0.5 & Main Deck (Frames 28 to 250) 1st Platform (Frames 18 to 126) 2nd Platform (Frames 78 to 158)	33 – 54 35 – 63 35 – 43
8	**Sonar Rm. #2 (AP ID – 77)** **2-18-0-Q**	0.5 & Main Deck (Frames 18 to 78) 1st Platform (Frames 18 to 78) 2nd Platform (Frames 18 to 78)	43 – 47 46 – 63 43 – 56
9	**Sonar Equip. Cooling Rm. (AP ID – 22)** **4-42-0-Q**	0.5 & Main Deck (Frames 42 to 78) 1st Platform (Frames 50 to 78) 2nd Platform (Frames 18 to 78) Hold (Frames 8 to 78)	27 – 40 30 – 44 30 – 44 35 – 63
10	**Forward IC Gyro (AP ID – 5F)** **4-94-0-C**	Main Deck (Frames 78 to 94) 1st Platform (Frames 78 to 94)	0 – 40 0 – 40

Table 2. WLAN Coverage Data

Hub #	Access Point Location & ID	Spaces with WLAN Coverage	Associated RSSI Values
		2nd Platform (Frames 78 to 126) Hold (Frames 42 to 126)	35 – 52 37 – 63
11	**Combat Systems Equip. Rm. #2 (AP ID – 1B)** **2-126-2-C**	Main Deck (Frames 78 to 164) 1st Platform (Frames 78 to 164) 2nd Platform (Frames 78 to 164) Hold (Frames 126 to 174)	0 – 45 39 – 63 0 – 42 0 – 36
12	**Auxiliary Machinery Rm. #1 (AP ID – 73)** **4-126-0-E**	Main Deck (Frames 78 to 174) 1st Platform (Frames 78 to 174) 2nd Platform (Frames 78 to 164) Hold (Frames 94 to 208)	28 – 45 0 – 48 32 – 55 32 – 63
13	**Main Engine Rm. #1 (AP ID – 2D)** **4-174-0-E**	Main Deck (Frames 126 to 220) 1st Platform (Frames 126 to 220) 2nd Platform (Frames 126 to 220) Hold (Frames 126 to 254)	0 – 55 0 – 43 0 – 43 30 – 63
14	**Chief Petty Officers Mess (AP ID – 42)** **1-174-0-L**	02 Level (Frames 154 to 174) 01 Level (Frames 163 to 200) Main Deck (Frames 78 to 300) 1st Platform (Frames 153 to 220)	0 – 35 40 – 50 28 – 63 43 – 50
15	**Sick Bay (AP ID – 29)** **1-220-3-L**	01 Level (Frames 158 to 200) Main Deck (Frames 42 to 338) 1st Platform (Frames 158 to 254) 2nd Platform (Frames 158 to 254) Hold (Frames 220 to 254)	37 – 42 28 – 63 0 – 43 0 – 43 0 – 43
16	**Supply Support Center (AP ID – 5B)** **3-220-2-Q**	01 Level Topside (Frames 118 to 240) Main Deck (Frames 206 to 258) 1st Platform (Frames 200 to 258) 2nd Platform (Frames 200 to 263) Hold (Frames 200 to 263)	36 – 48 0 – 48 35 – 60 40 – 63 40 – 60
17	**Supply Department Office (AP ID – 36)** **1-254-0-Q**	01 Level (Frames 300 to 330) Main Deck (Frames 220 to 330) 1st Platform (Frames 220 to 260) 2nd Platform (Frames 220 to 254) Hold (Frames 220 to 254)	0 – 40 20 – 63 0 – 46 0 – 40 0 – 40
18	**Main Engine Rm. #2 (AP ID – 21)** **4-254-0-F**	01/02 Levels (Frames 300 to 330) Main Deck (Frames 220 to 330) 1st Platform (Frames 254 to 300) 2nd Platform (Frames 254 to 300) Hold (Frames 254 to 300)	0 – 45 0 – 45 50 – 63 50 – 63 50 – 63
19	**Casualty Control Station (AP ID – 12)** **1-268-0-C**	04 Level (Frames 272 to 282) 03 Level (Frames 282 to 299) 02 Level (Frames 299 to 304) 01 Level (Frames 274 to 330)	0 – 45 46 – 54 48 – 58 48 – 58

Table 2. WLAN Coverage Data

Hub #	Access Point Location & ID	Spaces with WLAN Coverage	Associated RSSI Values
		01 Level – Topside (Fr. 118 – 240) Main Deck (Frames 220 to 338) 1st Platform (Frames 254 to 300) 2nd Platform (Frames 254 to 300) Hold (Frames 254 to 300)	0 – 38 0 – 57 0 – 48 0 – 48 0 – 48
20	**Radar Room #3 (AP ID – 6B)** **01-274-1-C**	04 Level (Frames 272 to 282) 03 Level (Frames 282 to 299) 02 Level (Frames 299 to 304) 01 Level (Frames 274 to 330) 01 Level – Topside (Fr. 240 – 300) Main Deck (Frames 220 to 338) 1st Platform (Frames 254 to 300) 2nd Platform (Frames 254 to 300) Hold (Frames 254 to 300)	0 – 46 40 – 46 48 – 58 48 – 63 0 – 35 0 – 55 0 – 40 0 – 40 0 – 40
21	**AFT IC Gyro (AP ID – 41)** **3-300-0-L**	Main Deck (Frames 300 to 338) 1st Platform (Frames 300 to 338) 2nd Platform (Frames 300 to 338) Hold (Frames 300 to 338)	40 – 50 0 – 57 30 – 63 35 – 43
22	**Shaft Alley (AP ID – 4A)** **5-300-01-E**	1st Platform (Frames 300 to 338) 2nd Platform (Frames 300 to 338) Hold (Frames 300 to 338)	0 – 45 0 – 50 55 – 63
23	**Combat Systems Equip. Rm. #3 Annex (AP ID – 72) 1-314-0-C**	Main Deck (Frames 254 to 338) 1st Platform (Frames 300 to 338) 2nd Platform (Frames 300 to 338)	20 – 63 32 – 50 32 – 48
24	**Crew Library/Learning Ctr. (AP ID – 67)** **2-338-2-L**	Main Deck (Frames 300 to 370) 1st Platform (Frames 300 to 370) 2nd Platform (Frames 300 to 370)	28 – 50 30 – 63 28 – 50
25	**Gas Turbine Generator Rm. #3 (AP ID – 1F)** **2-370-0-E**	1st Platform (Frames 370 to 410) 2nd Platform (Frames 370 – 432)) Hold (Frames 410 – 434)	30 – 63 20 – 63 20 – 40
26	**Tactas Hoist Room (AP ID – 4F)** **2-442-0-Q**	1st Platform (Frames 442 to 500) 2nd Platform (Frames 442 to 500)	45 – 63 30 – 48
27	**Deck Department Office (AP ID – 0E)** **2-450-2-Q**	Topside (Frames 366 to 500) 1st Platform (Frames 370 to 500) 2nd Platform (Frames 410 to 500)	0 – 52 28 – 63 30 – 40

TOPSIDE COVERAGE

The data is Table 2 shows Topside coverage from about Frame 30 back to Frame 300 and from Frame 366 to Frame 500. This is essentially ship-wide coverage Topside with a coverage gap by the Harpoon Launchers. It should be noted that Topside coverage is provided by WLAN Access Points installed within the ship whose emissions penetrate the ship's hull into Topside areas. As such Topside coverage signal strength is inconsistent. Specific Access Points providing Topside coverage are located in the following spaces:

- Bridge (Pilot House) -- 04-130-0-C
- Wardroom Passageway -- 02-154-2-Q
- Supply Support Center -- 3-220-2-Q
- Central Control Station (CCS) -- 1-268-0-C
- Radar Room 3 -- 01-274-1-C
- Deck Department Office – 2-450-2-Q

Further analysis of Topside coverage during the test period using the WLAN receiver revealed that the WLAN signal was not detectable at distances of 30 to 50ft outside the ship's hull. Additional data on this will be presented later in the report.

WLAN SUSCEPTIBILITY TEST RESULTS

Tests for susceptibility due to the WLAN were performed from April 1998 to July 1998. The tests focused on the impact of the WLAN on ships systems such as the Main Engines, Generators, Weapon Systems, Radars, Sensors, Microwave Devices, Medical Equipment, and Internal Communication devices. Events such as uncontrolled activation and/or deactivation were monitored as well as RF interference due to WLAN emissions. Specific attention was focused on the impact of WLAN emissions on engineering equipment due to problems encountered in earlier shipboard tests of the DC WIFCOM radios. Testing was performed while the ship was pier-side as well as while the ship was underway.

As part of the tests, WLAN Access Points were turned off and on with ship systems in operation with no indication of susceptibility. Further WLAN equipment (operating at 2.4 GHz with signal power of up to 500mW) was used consistently around the ship systems listed above with no indications of susceptibility. The effort involved using Wearable PCs equipped with WLAN Interface Cards and WLAN Access Points for significant periods in engineering and combat systems spaces. After more than five months of consistent WLAN operations aboard DDG 68, there have been NO reported incidents of WLAN susceptibility by any engineering, combat, communications, medical or other systems aboard the ship. These shipboard systems have also had NO impact on the WLAN.

WLAN DETECTABILITY (THREAT ANALYSIS) TEST RESULTS

The purpose of this test was to determine the range of WLAN emissions outside the hull and assess the feasibility of ship detectability and, hence, vulnerability due to such UHF emissions. The test frequency spectrum was 1.7 to 2.6 GHz. This spectrum included the 2.4 to 2.5 GHz band used by the WLAN. The tests were performed in cooperation with the SESEF in Mayport Florida in June 1998.

As DDG 68 sailed around within the basin at Mayport with WLAN devices shut down, a "Feed Horn" was used to measure ambient noise level in the 1.7 to 2.6 GHz spectrums. It should be noted that the doors between the Bridge and the Bridge Deck were left open during this effort. Once the baseline noise level had been established, and with the "Feed Horn" still trained on DDG 68, WLAN devices were turned on. The ship then sailed as close as possible to the SESEF (within three-tenths of a mile) while SESEF personnel attempted to measure variations from the baseline. With the ship within three-tenths of a mile, the "Feed Horn" detected no variations in the baseline. The ship was tracked as she sailed away, still with no

detectable WLAN emissions, for a distance of one mile. The lack of any detectable WLAN emissions after these tests led SESEF personnel to conclude that the WLAN posed NO threat to the ship's electronic signature. These results concurred with test results obtained by AEPTEC Microsystems personnel, which detected no WLAN emissions beyond 50ft of the ship's hull.

With regards to the ability of an external source to retrieve information from or impair the performance of the WLAN/SNAP LAN, tests revealed that any such efforts were only possible within 50ft of the ship's hull. Tests further revealed that such was not achievable as a result of inherent security within the WLAN. The inherent security hierarchy is as follows:

- The WLAN utilizes IEEE 802.11 Frequency Hopping Spread Spectrum technology and executes a unique hopping pattern across 78 non-overlapping frequencies. Its table of 66 hopping patterns (with 10 hops every second) greatly minimizes the probability that WLAN data can be collected.
- A specific Net Address is configured for all DDG 68 WLAN devices without which WLAN connection cannot be achieved. Neither will any information detected be useful as the data is scrambled prior to transmission and re-assembled at the target.
- The WLAN includes an address table that may be built to include the unique Ethernet address for all WLAN interface devices including the Wearable PCs. Any address outside this table will be automatically shut off from accessing the WLAN by the Access Points.